SSL - CVE-2019-1551

PUBLISHED: MARCH 4, 2020 | LAST UPDATE: : OCTOBER 15, 2021

SUMMARY

In December 2019, openssl.org released a security advisory [1] detailing an overflow bug in the x64_64 Montgomery squaring procedure issue. The following vulnerability may affect the TLS/SSL data plane of ACOS devices and is addressed in this document. The ACOS management plane can also be affected if the default keys are configured for 1024-bit RSA keys.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-1551	CVSS 3.0	4.8 Medium	openssl: Integer overflow in RSAZ modular exponentiation on x86_64 [2]

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to this vulnerability and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

Releases Affected			Releases Resolved or Unaffected
5.2.0	–	5.2.1	5.2.1-P1 (1)
5.0.0	–	5.1.0-P4	5.1.0-P5 (1)
5.0.1-TPS	–	5.0.2-TPS-Px (2)	None
4.1.4	–	4.1.4-GR1-P2	4.1.4-GR1-P3, 5.1.0-P3 (1)
4.1.1	–	4.1.1-P12	4.1.1-P13 (1)
3.2.3	–	3.2.5-Px (2)	None

(1) Resolved or unaffected releases apply to ACOS data plane service.

(2) Affects only ACOS management plane services, see workarounds and mitigations below.

WORKAROUNDS AND MITIGATIONS

ACOS DATA PLANE

None.

ACOS MANAGEMENT PLANE

Default keys for the ACOS management plane are 2048-bits, which are not exposed to this vulnerability. If 1024-bit RSA keys are generated or imported by the system administrator, they will be exposed to this issue.

Ensure that ACOS devices are configured for RSA keys support only for 2048-bits or greater key sizes.

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2019-1551	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t).

RELATED LINKS

Ref #	General Link
[1]	OpenSSL Security Advisory [6 December 2019]
[2]	NIST NVD, CVE-2019-1551

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2020-03-04	Initial Publication
1.1	2020-03-05	Typo correction
2.0	2021-08-16	Add resolved releases for 5.2.1, update 5.1.0
3.0	2021-10-15	Added consideration for ACOS management plane and ACOS TPS releases, including workarounds/mitigations to distinguish between management & data planes.